(vi)   providing an indication of anomalous network usage if the present usage as represented by the current signature deviates from that represented by the normal historic signature by more than a predetermined amount.

REMARKS

Objection under 35 USC § 132

The feature "accuracy measure" in claims 31, 32, 41 and 42 has not been removed from the claims as required by the Examiner since this feature is described in connection with Figure 15 on page 36 of the specification. In the second full paragraph of that page, it is explained that a measure of the detectors performance can be derived in the way set out in those claims. In this context, "performance" relates to the detection accuracy. Thus in the claims the term "accuracy" has been used in place of "performance".

In connection with the feature of retraining of the neural network set out in claims 33 and 43, this is also described in connection with Figure 15 on page 36 where it is explained that "once the performance falls below a certain predefined level, action can be taken to improve the performance . . . . This action involves retraining a neural network . . .".

Thus the Examiner's objection that new material has been added is respectfully traversed since no new material has been added.

Rejection under 35 USC § 101

The Examiner argues, in essence, that to claim statutory subject matter it is necessary to claim a process which transforms or reduce certain substances. It is noted that claims 1, 12,

13 and 22 (as amended) all claim the storing of information (or an apparatus equivalent) relating to the transmission of messages over an electronic transmission medium, the processing of the stored information to create a first signature, the processing of the stored information to create a second signature and the detection of anomalies by comparing the first and second signatures.

It is respectfully submitted that all of these acts are manipulation of specific data representing physical activities (i.e. the transmission of messages by an entity) and furthermore that the claims (as amended) relate to the transmission of these messages over an electronic transmission medium.

Thus it is submitted that the invention as explicitly recited in claims 1, 12, 13, 22 and 30 produces a concrete and tangible result in precisely the terms required by the precedents set out by the Examiner.

It is noted that no objection under 35 USC §101 has been raised by the Examiner against claim 40. Pending method claim 30 is drafted in similar terms to apparatus claim 40 and it is not clear why the Examiner finds claim 40 acceptable but claim 30 objectionable. Claim 30 has therefore been amended to emphasize the parallels between claims 30 and claim 40. Thus the comments given above in connection with the other independent claims apply equally to claim 30 and furthermore, claim 30 should be allowable under 35 USC §101 for the same reasons that claim 40 is allowable.

Rejection under 35 USC §103

The Examiner has cited Hunt and Gillick. As noted previously, both of these references teach voice recognition systems using statistical (but not neural network) analysis of

electronic signals representing voice wave forms. They are concerned with pattern matching and not with the detection of anomalies (commonly defined as irregularity of behaviour etc.). Indeed, matching voice patterns to a set of predetermined words which can be recognized by the apparatus of Hunt and Gillick is the opposite of the teaching of the present invention (which attempts to identify unknown irregularities in a stream of otherwise "normal" data).

Thus, Applicants question again whether the references cited by the Examiner have any relevance whatsoever to the invention explicitly recited in the pending claims. Applicants have made little comment below in connection with the Examiner's assertions about the prior art relevance to the dependent claims. This is because in most cases (and as explained in previous responses) the portions of the prior art selected by the Examiner bear no relationship to the technical features claimed in the identified dependent claims. Thus for all those dependent claims for which there is no explicit comment below, Applicants merely state that the Examiner's objections have no technical relevance to those claims and that counter-argument is therefore impossible.

In connection with claim 1, as noted above, Hunt et al does not disclose a method of detecting anomalies (rather it discloses a method of recognizing particular speech patterns by matching incoming speech input with a set of known wave form definitions).

Examiner asserts that Hunt et al at column 8, lines 9-54 discloses the detection of anomalies. This is not so. The portion of the specification referred to by Examiner (and indeed the whole of the rest of the Hunt specification) discloses pattern matching. It does not disclose the detection of anomalies. The whole thrust of Hunt is to detect spoken digits. This is achieved by pre-programming Hunt with digit patterns during a testing phase in which a user speaks into the system described in Hunt. Thereafter, the Hunt system simply provides a yes/no/maybe response. There is no concept of monitoring a flow of messages, accepting

gradual changes in this flow but highlighting any unusual occurrences (as defined in the invention as recited in claim 1).

Thus, Applicant does not agree with the Examiner's interpretation of Hunt in relation at least to features (v) and (vi) of claim 1.

Furthermore, the Examiner admits that features (iii) and (iv) of claim 1 are not disclosed in Hunt et al. The Examiner suggests that claim 5 of Gillick discloses these features. This is incorrect.

Features (iii) and (v) of claim 1 of the present application describe the creation of a second signature which relates to messages transmitted over a period shorter than that of the first signature and more recent than the first signature. Thus the second signature is a short term recent signature whereas the first signature is a longer term historic signature. The longer term historic signature is updated with a weighted average from the shorter term, more recent signature.

However, in the Gillick system the operation is very different. During training of the speech recognition system of Gillick, "probabilistic acoustic cluster models" are stored "to represent at least a part of more than one vocabulary word" (see lines 33-36 of claim 5). Thus "cluster models" are stored historic long term voice recognition patterns. At line 50 of claim 5, it is explained that an acoustic description of said utterance is received as "a sequence of individual frames" and that comparing the utterances with the cluster models includes "deriving a series of smooth frames from said sequence of individual frames". Thus in Gillick, the recent data is averaged in order to compare it with the historic cluster models. There is no updating of the cluster models (feature (iv) of pending claim 1 of the present application) and furthermore, Gillick proposes using an averaged recent signature for voice

recognition detection (which in the Examiner's interpretation – which is not accepted by Applicant – means that Gillick uses an averaged "second signature" for "anomaly detection") which is at odds with features (v) and (vi) of present claim 1..

Thus, in summary, (and using the Examiner's interpretation of the prior art which is not accepted by Applicant), Gillick performs no updating of the first signature and uses an averaged second signature solely for anomaly detection.

Thus even if it were permissible to choose selected portions of Hunt and Gillick, and using hindsight, attempt to combine these two teachings to arrive at the invention recited in claim 1, a skilled artisan performing such an unlikely combination would still not arrive at the claimed invention. Thus it is submitted that the Examiner has failed to show that claim 1 would have been obvious in view of a combination of Hunt and Gillick.

In connection with claim 8, it is noted yet again that Hunt does not disclose a neural network. The portion referred to by the Examiner repeatedly over previous Office Actions as well as the present Office Action refers simply to statistical analysis. The equations shown in the portion referred to by the Examiner do not define a neural network.

The remaining dependent claims are non-obvious at least by virtue of their dependency from claim 1.

In connection with the Examiner's arguments concerning claims 12 and 13, these arguments are the same as those propounded against claim 1. Thus for the same reasons given above, Applicant submits that claims 12 and 13 are non-obvious.

The Examiner does not appear to have raised an obviousness objection against claims 14 to 18.

In connection with claim 19, it is noted that Hunt et al does not disclose the use of a neural network.

In connection with the remaining dependent claims depending from claim 12, the same comments given above apply.

Claim 23 recites "a method of deriving potential fraudulent telephone calls from information relating to telephone calls . . . ".

The Examiner suggests that such a method can be achieved by the skilled artisan by selectively combining components of two prior art voice recognition systems. Applicant does not agree.

For the reasons stated above, the combination suggested by the Examiner is unworkable and does not fully disclose the invention even as broadly recited in claim 1. It certainly does not allow the skilled artisan to arrive at a method of deriving potential fraudulent telephone calls. The combination of prior art teaching relating to voice recognition will inevitably result in a voice recognition system and not in a system capable of detecting fraudulent telephone calls.

The Examiner is apparently ignoring the recitation of claim 23 and simply reiterating the arguments produced in connection with claims 1 and 12.

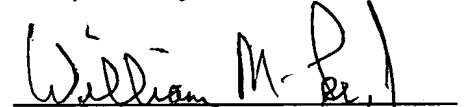For all the reasons given above, the rejection of claim 23 is traversed.

Similarly, claims 24 to 29 are, it is submitted, non-obvious for all the reasons given above and at least by virtue of their dependency from claim 23.

The arguments raised by the Examiner in connection with claims 30 and 40 and their respective dependent claim sets are the same as those used in connection with the other independent and dependent claims. Thus Applicants' arguments are the same. For at least the reasons given above, claims 30 to 45 are, it is submitted, non-obvious.

Given the above, it is submitted that this response should be entered since the amendments deal with the 35 USC §101 issue. Furthermore, as explained it is submitted that the claims are allowable over the prior art. Allowance is thus solicited.

Date: August 16, 2001

Respectfully submitted,

William M. Lee, Jr.
Lee, Mann, Smith, McWilliams,
Sweeney & Ohlson.
P.O. Box 2786
Chicago, Illinois 60690-2786
Direct Line 312-368-6620
Telephone   312-368-1300
Facsimile 312-368-0034

1.   (four times amended) A method of detecting anomalies in messages transmitted

electronically by an entity over an electronic transmission medium comprising the steps of:

(i)   storing information relating to the transmission of messages by the entity over a given time

period,

(ii)   processing the stored information to create a first signature comprising a plurality of

parameters related to the transmission of messages over that time period wherein the

parameters comprise at least one parameter related to the transmission of messages over

a portion of the period and also related to the position of the portion in the period, to

enable output data to be derived from the stored information;

(iii)   processing the stored information to create a second signature comprising a plurality of

parameters related to the transmission of messages over a second period shorter than the

first and more recent than the first;

(iv)   updating the first signature by a weighted averaging with the second signature;

(v)   detecting anomalies by inputting the signatures to the anomaly detector; and

(vi)   processing the signatures using the anomaly detector to derive the anomalies by detecting

unexpected patterns in the transmission of messages by the entity over the time period.

12.   (four times amended) A computer system for detecting anomalies in messages transmitted

over an electronic transmission medium by an entity comprising:

(i)   a data store arranged to store information relating to the transmission of messages by the

entity over a given time period,

(ii)   an input arranged to receive information about each of a number of events which occurred

during the time period;

(iii) a processor arranged to convert the information into a signature comprising a plurality of parameters related to the transmission of messages over the time period wherein the parameters comprise at least one parameter related to the transmission of messages over a portion of the period and also related to the position of the portion in the period, to enable output data to be derived from the stored information and wherein said processor is further arranged to convert at least part of the information into a second signature, comprising a plurality of parameters related to the transmission of messages over a second period, shorter than the first and more recent than the first; and also to update the first signature by a weighted averaging with the second signature;

(iv) an anomaly detector;

(v) an input arranged to provide the signatures to the anomaly detector; the anomaly detector being arranged to process the signatures to derive the anomalies by detecting unexpected patterns in the transmission of messages by the entity over the time period.

13. (four times amended) A method of deriving anomalies from messages transmitted electronically by an entity over an electronic transmission medium over time, comprising the steps of:

(i) creating a first signature comprising a plurality of parameters related to the transmission of messages over a predetermined first time period;

(ii) creating a second signature comprising a plurality of parameters related to the transmission of messages over a second period shorter than the first and more recent than the first;

(iii) updating the first signature by a weighted averaging with the second signature;

(iv) inputting the signatures to the anomaly detector; and

(v) detecting anomalies by processing the signatures using the anomaly detector to derive the

anomalies by detecting unexpected patterns in the transmission of messages by the entity over the time period.

22. (four times amended) A computer system for detecting anomalies in messages transmitted by an entity <u>over an electronic transmission medium</u> over time, the system comprising:

an input arranged to receive information about the transmission of messages by the entity;

a processor arranged to create a first signature comprising a plurality of parameters related to the transmission of messages over a predetermined first time period and to create a second signature comprising a plurality of parameters related to the transmission of messages over a second period shorter than the first and more recent than the first;

a processor arranged to calculate a weighted averaging of the first and second signatures to form an updated first signature;

an anomaly detector;

an input arranged to provide the signatures to the anomaly detector; and

wherein said anomaly detector is arranged to process the signatures to derive the anomalies by detecting unexpected patterns in the transmission of message by the entity over the time period.

30. (amended) A method of detecting anomalous usage of a network comprising:-

(i)   monitoring traffic flowing in the network,

(ii)   <u>processing the monitored traffic to</u> generate<u>e</u>[ing] a normal historic signature and a stored historic signature each representative of network usage over a first time period,

(iii) <u>processing the monitored traffic to</u> generate<u>e</u>[ing] a current signature representative of network usage over a second time period which is shorter and more recent than

the first time period,

(iv)   comparing the current and normal historic signatures to determine[ing] whether the

current signature represents normal usage by comparing it with the normal historic

signature,

(iv)   if the current signature is determined to represent normal usage, producing an

updated stored historic signature by combining the stored historic signature and the

current signature using a weighted averaging procedure so that consistent trends

present in the current signature are gradually over time introduced into the longer

term trends incorporated in the stored historic signature,

(vi)   providing an indication of anomalous network usage if the present usage as

represented by the current signature deviates from that represented by the

normal historic signature by more than a predetermined amount.